UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/081,500	02/22/2002	John Owlett	GB920010095US1	1505

26502 7590 08/09/2005

IBM CORPORATION
IPLAW IQ0A/40-3
1701 NORTH STREET
ENDICOTT, NY 13760

EXAMINER	
LAFORGIA, CHRISTIAN A	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 08/09/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/081,500	OWLETT, JOHN	
	Examiner	Art Unit	
	Christian La Forgia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 November 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 February 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-14 have been presented for examination.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-5 and 11-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Application Publication No. 2002/0034301 to Andersson, hereinafter Andersson, in view of U.S. Application Publication No. 2004/0202328 to Hara.

4. As per claims 1, 13, and 14, Andersson discloses a method for authentication of a user by an authenticating entity comprising the steps of:

the authenticating entity sending a challenge to the user (page 3, paragraph [0040], i.e. the authentication server issues a challenge to the user);

the user encrypting the challenge using a private key of an asymmetric key pair (page 3, paragraph [0040], i.e. the authentication token encrypts the challenge with the user's private key);

the user sending a response to the authenticating entity in the form of the encrypted challenge (page 3, paragraph [0040], i.e. the authentication token encrypts the challenge with the user's private key, and returns it to the authentication server).

5. Andersson does not disclose the user adding a spoiler to the challenge and encrypting the combined spoiler and challenge.

6. Hara discloses adding padding to data and encrypting the data and the padding information (Figures 7b, 7c, page 5, paragraphs [083], [0084]).

7. It would have been obvious to one of ordinary skill in the art at the time the invention was made to add padding data to the password and encrypting the password with the padding data, since Hara discloses at page 5, paragraphs [083], [0084] that padding data makes it better suited for encryption, as it is known that padding data to a certain length makes the encryption stronger, which is desirable when trying to prevent transmitted password information from being intercepted.

8. Regarding claim 2, Andersson teaches wherein the method includes the authenticating entity decrypting the encrypted combined spoiler and challenge using the public key of the asymmetric key pair and determining if the user has been authenticated (page 3, paragraph [0040], i.e. the returned challenge is then decrypted by the authentication server with the user's public key).

9. Regarding claim 3, Hara teaches wherein the addition of spoiler to the challenge is carried out by applying spoiler function to the challenge (Figures 7b, 7c, page 5, paragraphs [083], [0084]).

10. With regards to claim 4, Hara teaches wherein the form the spoiler function is sent to the authenticating entity (Figures 7b, 7c, page 5, paragraphs [0084], i.e. knowing where the padding is located in order for it to be removed later).

11. Regarding claim 5, Hara discloses wherein the spoiler is added to the challenge as a prefix or a suffix and the authenticating entity extracts the challenge by counting the number of bytes from the beginning or end of the combined spoiler and challenge (page 5, paragraphs [0084]).

12. Regarding claim 11, Andersson teaches wherein the challenge is a bit sequence (page 1 paragraph [0007], i.e. Wireless Application Protocol transmits data in binary sequence).

13. Regarding claim 12, Hara discloses wherein the spoiler is an additional bit sequence (page 5, paragraphs [083], [0084]).

14. Claims 6-8 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Andersson in view of Hara as applied above, and further in view of U.S. Patent No. 6,072,875 to Tsudik, hereinafter Tsudik.

15. Regarding claim 6, Andersson and Hara do not wherein the method includes the user obtaining a digest of the combined spoiler and challenge before the step of encrypting.

16. Tsudik teaches wherein the method includes the user obtaining a digest of the challenge before the step of encrypting (column 3, line 59 to column 4, line 11).

17. It would have been obvious to one of ordinary skill in the art at the time the invention was made to obtain a digest of the combined spoiler and challenge, since Tsudik states at column

4, lines 12-21 that such a modification would allow for mobile users while minimizing the traceability and possibility of identifying the mobile user.

18. With regards to claim 7, Tsudik discloses wherein the user obtains the digest by applying a hash function to the combined spoiler and challenge (column 3, line 59 to column 4, line 11).

19. With regards to claim 8, Tsudik teaches wherein the user sends details of the spoiler and the method of obtaining the digest to the authenticating entity (column 6, lines 42-63, i.e. home domain authority keeps track of user).

20. Regarding claim 9, Tsudik teaches wherein the user sends details of the algorithm used for encryption to the authenticating entity (column 5, lines 27-48).

21. It would have been obvious to one of ordinary skill in the art at the time the invention was made to send details of the encryption to be used by mobile users, since Tsudik states at column 4, lines 12-21 that such a modification would allow for mobile users while minimizing the traceability and possibility of identifying the mobile user.

22. Concerning claim 10, Tsudik discloses wherein the authenticating entity obtains a digest of the combined spoiler and the original challenge that the authenticating entity sent to the user and compares the digest a digest obtained by decrypting the response from the user (column 3, line 59 to column 4, line 11).

Conclusion

23. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

24. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

25. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christian LaForgia
Patent Examiner
Art Unit 2131

clf